IEEE *Xplore*

Welcome United States Patent and Trademark Office

Search Results   BROWSE   SEARCH   IEEE XPLORE GUIDE

Results for "((pcr<in>metadata) <or> (mpeg<in>metadata))<and> (digital signature&l..."   ⊠e-mail
Your search matched **4** of **1255513** documents.
A maximum of **100** results are displayed, **25** to a page, sorted by **Relevance** in **Descending** order.

» Search Options

View Session History

New Search

» Key

IEEE JNL	IEEE Journal or Magazine
IEE JNL	IEE Journal or Magazine
IEEE CNF	IEEE Conference Proceeding
IEE CNF	IEE Conference Proceeding
IEEE STD	IEEE Standard

Modify Search

((pcr<in>metadata) <or> (mpeg<in>metadata))<and> (digital signature<in>metad 🔳

☐ Check to search only within this results set

Display Format: ⦿ Citation   ○ Citation & Abstract

Select   Article Information

☐   1. **Authentication of MPEG-4-based surveillance video**
Pramateftakis, A.; Oelbaum, T.; Diepold, K.;
Image Processing, 2004. ICIP '04. 2004 International Conference on
Volume 1, 24-27 Oct. 2004 Page(s):33 - 37 Vol. 1
Digital Object Identifier 10.1109/ICIP.2004.1418683

AbstractPlus | Full Text: PDF(634 KB)   **IEEE CNF**

☐   2. **Wireless multimedia error resilience via a data hiding technique**
Chun-Shien Lu;
Multimedia Signal Processing, 2002 IEEE Workshop on
9-11 Dec. 2002 Page(s):316 - 319

AbstractPlus | Full Text: PDF(446 KB)   **IEEE CNF**

☐   3. **An MPEG tolerant authentication system for video data**
Uehara, T.; Safavi-Naini, R.; Ogunbona, P.;
Multimedia and Expo, 2004. ICME '04. 2004 IEEE International Conference on
Volume 2, 27-30 June 2004 Page(s):891 - 894 Vol.2

AbstractPlus | Full Text: PDF(649 KB)   **IEEE CNF**

☐   4. **Secure representation of multimedia content licenses**
Sanmartino, A.; Perramon, X.; Delgado, J.;
Web Delivering of Music, 2004. WEDELMUSIC 2004. Proceedings of the Four
Conference on
2004 Page(s):85 - 91
Digital Object Identifier 10.1109/WDM.2004.1358104

AbstractPlus | Full Text: PDF(291 KB)   **IEEE CNF**

View Selected Items

Help   Contact Us   Privacy & :

Indexed by
Inspec

THE ACM DIGITAL LIBRARY

Published before March 2001
Terms used **digital** **signature** **MPEG** **PCR**

Found **3,381** of **116,122**

Sort results by	relevance ▼	● Save results to a Binder	Try an Advanced Search
Display results	expanded form ▼	? Search Tips	Try this search in The ACM Guide
		☐ Open results in a new window	

1 Papers: On the validity of digital signatures

Jianying Zhou, Robert Deng
April 2000 **ACM SIGCOMM Computer Communication Review**, Volume 30 Issue 2

Publisher: ACM Press

Full text available: 📄 pdf(586.65 KB)   Additional Information: full citation, abstract, references

An important feature of digital signatures is to serve as non-repudiation evidence. To be eligible as non-repudiation evidence, a digital signature on an electronic document should remain valid until its expiry date which is specified by some non-repudiation policy. As signature keys may be compromised and the validity of signatures may become questionable, additional security mechanisms need to be imposed on digital signatures. This paper examines the mechanisms for maintaining the validity of ...

Keywords: digital signature, non-repudiation, secure electronic commerce

2 Digital signatures: can they be accepted as legal signatures in EDI?

Patrick W. Brown
December 1993 **Proceedings of the 1st ACM conference on Computer and communications security**

Publisher: ACM Press

Full text available: 📄 pdf(809.34 KB)   Additional Information: full citation, abstract, references, citings, index terms

Digital Signature (DS) technology may be employed to produce legally enforceable signatures in Electronic Data Interchange (EDI) among computer users within the same general guidelines and requirements as those developed for handwritten signatures on paper. Digital signature technology promises assurance at least equal to written signatures. From a legal standpoint, this assurance remains to be tested in the evidentiary process. Business policies for organizational use of this technology ar ...

Keywords: EDI, cryptography, digital signatures, distributed systems, law

3 Digital signatures for flows and multicasts

Chung Kei Wong, Simon S. Lam
August 1999 **IEEE/ACM Transactions on Networking (TON)**, Volume 7 Issue 4

Publisher: IEEE Press
Full text available: pdf(268.97 KB)   Additional Information: full citation, references, citings, index terms

4 Structural digital signature for image authentication: an incidental distortion resistant scheme
Chun-Shien Lu, Hong-Yuan Mark Liao
November 2000 **Proceedings of the 2000 ACM workshops on Multimedia**
Publisher: ACM Press

Full text available: pdf(684.69 KB)   Additional Information: full citation, abstract, references, citings, index terms

The existing digital data authentication methods are able to detect tampered regions, but are too fragile to resist incidental distortions. This paper will present a new digital signature scheme for image authentication by making use of image content (in the wavelet domain). Based on this concept, a structural digital signature (*SDS*) is constructed. *SDS* is a signature that can be used to judge whether an incoming modification is incidental or malicious. When the structure of an ...

Keywords: authentication, digital signature, fragility, robustness, wavelet transform

5 Efficient verifiable encryption (and fair exchange) of digital signatures
Giuseppe Ateniese
November 1999 **Proceedings of the 6th ACM conference on Computer and communications security**
Publisher: ACM Press

Full text available: pdf(781.40 KB)   Additional Information: full citation, abstract, references, citings, index terms

A fair exchange protocol allows two users to exchange items so that either each user gets the other's item or neither user does. In [2], verifiable encryption is introduced as a primitive that can be used to build extremely efficient fair exchange protocols where the items exchanged represent digital signatures. Such protocols may be used to digitally sign contracts.This paper presents new simple schemes for verifiable encryption of digital signatures. We make us ...

Keywords: contract signing problem, digital signatures, fair exchange, proof of knowledge, public-key cryptography, verifiable encryption

6 Business: The 8th layer: Will the digital signature transform e-commerce?
Kate Gerwig
September 2000 **netWorker,** Volume 4 Issue 3
Publisher: ACM Press
Full text available: pdf(502.72 KB)
html(13.80 KB)   Additional Information: full citation, index terms

7 The digital signature standard
CORPORATE NIST
July 1992 **Communications of the ACM,** Volume 35 Issue 7
Publisher: ACM Press
Full text available: pdf(3.12 MB)   Additional Information: full citation, references, citings, index terms

8 A method for obtaining digital signatures and public-key cryptosystems

R. L. Rivest, A. Shamir, L. Adleman
February 1978 **Communications of the ACM**, Volume 21 Issue 2
Publisher: ACM Press

Full text available: pdf(748.63 KB)   Additional Information: full citation, abstract, references, citings, index terms

An encryption method is presented with the novel property that publicly revealing an encryption key does not thereby reveal the corresponding decryption key. This has two important consequences: (1) Couriers or other secure means are not needed to transmit keys, since a message can be enciphered using an encryption key publicly revealed by the intented recipient. Only he can decipher the message, since only he knows the corresponding decryption key. (2) A message can be "signed" ...

Keywords: authentication, cryptography, digital signatures, electronic funds transfer, electronic mail, factorization, message-passing, prime number, privacy, public-key cryptosystems, security

9 Digital signature schemes for computer communication networks

Henk Meijer, Selim Akl
October 1981 **ACM SIGCOMM Computer Communication Review , Proceedings of the seventh symposium on Data communications SIGCOMM '81**, Volume 11 Issue 4
Publisher: ACM Press

Full text available: pdf(338.40 KB)   Additional Information: full citation, abstract, references, citings, index terms

This paper introduces four new digital signature schemes for computer communication networks. These involve one or more arbitrators who validate and authenticate messages and signatures without having access to the actual contents of the messages.

Keywords: Arbitration, Cryptology, Digital signature

10 Digital signatures with RSA and other public-key cryptosystems

Dorothy E. Denning
April 1984 **Communications of the ACM**, Volume 27 Issue 4
Publisher: ACM Press

Full text available: pdf(374.39 KB)   Additional Information: full citation, references, citings, index terms

Keywords: cryptanalysis, cryptographic, hashing, homomorphism, protocol

11 On digital signatures

Jerome H. Saltzer
April 1978 **ACM SIGOPS Operating Systems Review**, Volume 12 Issue 2
Publisher: ACM Press

Full text available: pdf(242.17 KB)   Additional Information: full citation, references, citings

12

Sorting out signature schemes
Birgit Pfitzmann
December 1993 **Proceedings of the 1st ACM conference on Computer and communications security**
Publisher: ACM Press

Full text available: pdf(1.19 MB)   Additional Information: <u>full citation</u>, <u>abstract</u>, <u>references</u>, <u>citings</u>, <u>index terms</u>

Digital signature schemes are a fundamental tool for secure distributed systems. It is important to have a formal notion of what a secure digital signature scheme is, so that there is a clear interface between designers and users of such schemes. A definition that seemed final was given by Goldwasser, Micali, and Rivest in 1988, and although most signature schemes used in practice cannot be proved secure with respect to it, they are all built so that they hopefully fulfil it, e.g., by the i ...

13 Pseudo-random testing and signature analysis for mixed-signal circuits
Chen-Yang Pan, Kwang-Ting Cheng
December 1995 **Proceedings of the 1995 IEEE/ACM international conference on Computer-aided design**
Publisher: IEEE Computer Society
Full text available: pdf(88.30 KB)
Publisher Site   Additional Information: <u>full citation</u>, <u>abstract</u>, <u>references</u>, <u>index terms</u>

In this paper, we address the problem of functional testing of mixed-signal circuits using pseudo-random patterns. By embedding the linear, time-invariant (LTI) analog circuit between a digital-to-analog converter (DAC) and an analog-to-digital converter (ADC), we can model the analog and converter circuitry as a digital LTI system and test it using the pseudo-random vectors. We give mathematical analysis and formulate the pseudo-random testing process as the linear transformation of a random pr ...

Keywords: Pseudo-Random Testing, Random Process, Signature Analysis, Impulse Response

14 Archival storage for digital libraries
Arturo Crespo, Hector Garcia-Molina
May 1998 **Proceedings of the third ACM conference on Digital libraries**
Publisher: ACM Press
Full text available: pdf(1.32 MB)   Additional Information: <u>full citation</u>, <u>references</u>, <u>citings</u>, <u>index terms</u>

15 Proxy signatures for delegating signing operation
Masahiro Mambo, Keisuke Usuda, Eiji Okamoto
January 1996 **Proceedings of the 3rd ACM conference on Computer and communications security**
Publisher: ACM Press
Full text available: pdf(1.18 MB)   Additional Information: <u>full citation</u>, <u>references</u>, <u>citings</u>, <u>index terms</u>

16 A digital multisignature scheme using bijective public-key cryptosystems
Tatsuaki Okamoto
November 1988 **ACM Transactions on Computer Systems (TOCS)**, Volume 6 Issue 4
Publisher: ACM Press

Full text available: Additional Information: <u>full citation</u>, <u>abstract</u>, <u>references</u>, <u>citings</u>, <u>index</u>

pdf(640.51 KB)   terms, review

A new digital multisignature scheme using bijective public-key cryptosystems that overcomes the problems of previous signature schemes used for multisignatures is proposed. The principal features of this scheme are (1) the length of a multisignature message is nearly equivalent to that for a singlesignature message; (2) by using a one-way hash function, multisignature generation and verification are processed in an efficient manner; (3) the order of signing is not restricted; and (4) this s ...

17 Simple forward-secure signatures from any signature scheme

Hugo Krawczyk
November 2000 **Proceedings of the 7th ACM conference on Computer and communications security**
Publisher: ACM Press
Full text available: pdf(231.13 KB)   Additional Information: full citation, references, citings, index terms

18 Preserving digital information forever

Andrew Waugh, Ross Wilkinson, Brendan Hills, Jon Dell'oro
June 2000 **Proceedings of the fifth ACM conference on Digital libraries**
Publisher: ACM Press
Full text available: pdf(115.99 KB)   Additional Information: full citation, abstract, references, index terms

Well within our lifetime we can expect to see most information being created, stored and used digitally. Despite the growing importance of digital data, the wider community pays almost no attention to the problems of preserving this digital information for the future. Even within the archival and library communities most work on digital preservation has been theoretical, not practical, and highlights the problems rather than giving solutions. Physical libraries have to preserve information ...

Keywords: archiving, digital preservation

19 A compact and fast hybrid signature scheme for multicast packet authentication

Pankaj Rohatgi
November 1999 **Proceedings of the 6th ACM conference on Computer and communications security**
Publisher: ACM Press
Full text available: pdf(759.34 KB)   Additional Information: full citation, abstract, references, citings, index terms

This paper proposes a compact and fast hybrid signature scheme that can be used to solve the problem of packet source authentication for multicast. This scheme can be viewed as an improvement to off-line/on-line signature schemes, in that the signature size overhead is much smaller. Since this is a generic technique, it should have applications to several other practical problems as well.

20 Meta-ElGamal signature schemes

Patrick Horster, Holger Petersen, Markus Michels
November 1994 **Proceedings of the 2nd ACM Conference on Computer and communications security**
Publisher: ACM Press
Full text available: pdf(1.16 MB)   Additional Information: full citation, abstract, references, citings, index terms

There have been many approaches in the past to generalize the ElGamal signature scheme. In this paper we integrate all these approaches in a Meta-ElGamal signature

scheme. We also investigate some new types of variations, that haven't been considered before. By this method we obtain in our example settings numerous variants of the ElGamal scheme. From these variants, we can extract new, highly efficient signature schemes, which haven't been proposed before. As an example, we present efficie ...

Results 1 - 20 of 200   Result page: **1**   2   3   4   5   6   7   8   9   10   next

Useful downloads: Adobe Acrobat   QuickTime   Windows Media Player   Real Player

L20	23	L19 and (digital near signature)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/11/11 23:38
L21	366	725/136.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/11/11 23:38
L22	4	L21 and (digital near signature)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/11/11 23:38
L23	515	725/135.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/11/11 23:39
L24	7	L6 and (digital near signature)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/11/11 23:39
L25	394	(380/54).CCLS.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/11/11 23:45
L26	499	(705/59).CCLS.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/11/11 23:45

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	412	348/231.99	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/11/11 23:35
L2	354	348/461.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/11/11 23:35
L3	233	348/152.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/11/11 23:35
L4	212	(348/231.6).CCLS.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/11/11 23:35
L5	878	(348/207.99).CCLS.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/11/11 23:36
L6	515	725/135.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/11/11 23:36
L7	1340	(714/758).CCLS.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/11/11 23:36
L8	0	L7 and ((digital near signature) and (MPEG))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/11/11 23:36
L9	1533	(713/176).CCLS.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/11/11 23:36

L10	255	L9 and MPEG	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/11/11 23:36
L11	1533	(713/176).CCLS.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/11/11 23:37
L12	255	L9 and MPEG	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/11/11 23:37
L13	251	(380/241).CCLS.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/11/11 23:44
L14	664	(380/201).CCLS.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/11/11 23:37
L15	201	(380/200).CCLS.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/11/11 23:37
L16	109	(380/212).CCLS.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/11/11 23:37
L17	132	(380/217).CCLS.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/11/11 23:38
L18	76	(380/221).CCLS.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/11/11 23:38
L19	628	725/31.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/11/11 23:38